Nad vládním návrhem zákona o kybernetické bezpečnosti
On the Government Bill of Cybernetic Security Act

Jiří Fuchs

Abstrakt: Tento článek se zamýšlí nad vládním návrhem zákona o kybernetické bezpečnosti, který projednává parlament. Nejdříve poukazuje na nezbytnost zajištění kybernetické bezpečnosti a na evropské a historické souvislosti návrhu. Poté popisuje zásady, ze kterých návrh vychází, a klíčové instituty, jež do právního řádu zavede. Na závěr pak věnuje pozornost některým úskalím, jež lze v návrhu nalézt.

Klíčová slova: Kybernetická bezpečnost, kyberprostor, Národní bezpečnostní úřad, kritická informační infrastruktura, stav kybernetického nebezpečí

Abstract: This article reflects upon the Government Bill of Cybernetic Security Act debated upon by the Parliament. It starts with pointing out to the necessity of ensuring cybernetic security and to the European and historical aspects of the Bill. Subsequently, it describes principles, on which the Bill is based, and key institutes, which the Bill is to introduce. Finally, it pays attention to certain problems, which may be identified in the Bill.

Keywords: Cybernetic security, cyberspace, National Security Bureau, critical information infrastructure, state of cybernetic danger

JEL Classification: K10, K23, K32

Úvod

V době, kdy píši tento článek (duben 2014), projednává parlament ve druhém čtení vládní návrh zákona o kybernetické bezpečnosti. Pojednávat o návrhu, který dosud nebyl schválen a nestal se platným právem, se může jevit jako předčasné. Nicméně dostupné informace zřetelně ukazují, že v parlamentu se potřebná politická vůle k přijetí návrhu najde a že návrh významných změn nedozná. Tento článek přitom využívá jednu výhodu, kterou disponuje doktrinální výklad, tedy výklad podávaný právní naukou. Na rozdíl od výkladu soudního není svázán s konkrétními skutkovými podstatami a může tak soudní výklad předbíhat. Právní norma může být předmětem doktrinálního výkladu ještě předtím, než se stane platným právem. Ostatně žádný problém nezmizí na základě toho, že se o něm „zatím" mluvit nebude. V neposlední řadě jsem přesvědčen, že i v případě nepřijetí vládního návrhu zákona o kybernetické bezpečnosti tento článek skromně přispěje k rozvoji poznání, protože může posloužit jako příspěvek do pokračující diskuse o potřebě zajistit v České republice kybernetickou bezpečnost.

V článku nejdříve poukážu na naléhavost potřeby zajistit kybernetickou bezpečnost, poté krátce nastíním evropské a historické souvislosti vládního návrhu a posléze přejdu k podstatě věci, tedy k obsahu vládního návrhu zákona o kybernetické bezpečnosti. Představím zásady, ze kterých návrh vychází, stručně popíši nejdůležitější instituty, které návrh do českého právního řádu zavede, a na závěr se pokusím zamyslet nad některými úskalími, jež lze v návrhu identifikovat.

1. Proč je potřeba zajistit kybernetickou bezpečnost

Základní funkcí státu je zajistit bezpečnost člověka a celé národní lidské společnosti[1]. Bezpečnost přitom představuje jednu z ústředních antropocentrických kategorií a tvoří základ pro každou lidskou činnost. Jedná se přitom o pojem s velmi širokým záběrem a mnohoznačnou problematikou. Lze jej vymezit jako objektivní stav spočívající v neexistenci ohrožení, tedy neexistenci nebezpečí ztráty něčeho cenného. Bezpečnost je jednou základních potřeb člověka, ale též společenských skupin a státu.[2]

Vědecko-technický pokrok přináší stále nové možnosti rozvoje lidské společnosti i každého člověka, současně ovšem poskytuje nové prostředky těm, kteří chtějí stát či společnosti nějakým způsobem zasáhnout. Státní moc tak v současnosti musí reagovat na nové bezpečnostní hrozby.

1) K tomu viz např. PROCHÁZKOVÁ, D. Bezpečnost, krizové řízení a udržitelný rozvoj. Praha: Univerzita Jana Amose Komenského Praha, 2010, s. 30.
2) K tomu viz např. DWORZECKI, Jacek. Bezpečnost státu jako součást udržitelného rozvoje. In BÍLÝ, J. a kol. Veřejná správa a bezpečnost státu jako součást udržitelného rozvoje. České Budějovice: Vysoká škola evropských a regionálních studií, 2013, s. 97 – 98.

Rozvoj informačních a komunikačních systémů umožňuje, aby se lidské aktivity přenášely z reálného světa do kybernetického prostoru. Vládní návrh zákona o kybernetické bezpečnosti vymezuje pojem kybernetického prostoru jako digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací (§ 2 písm. a).[3] Ačkoliv neexistuje všeobecně uznávaná definice kyberprostoru, pojetí tohoto pojmu ve vládním návrhu v zásadě odpovídá současnému stavu poznání.

Pojem kyberprostor poprvé požil v roce 1982 americko-kanadský spisovatel W. Gibson ve své povídce Burning Chrome. Podrobněji pak kyberprostor popsal ve svém románu Neuromancer (1984), a to jako konsensuální datovou halucinaci vizualizovanou v podobě imaginárního prostoru, jenž tvoří počítačově zpracovaná data a jenž je přístupný pouze vědomí, nikoliv fyzické tělesnosti uživatelů.[4] Současná česká nauka pojem kyberprostoru zpravidla chápe jako nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. Kyberprostor umožňuje vytváření, uchovávání, využívání a výměnu informací. Zahrnuje počítače a databáze propojené komunikačními systémy, například celosvětovou síť internet, a využívá nové možnosti komunikace, jako jsou například emaily, webové stránky, počítačové sítě, telefony, faxy a videokonference.[5] Kyberprostor se vyznačuje imateriálností a deteritorialitou. Někdy se poukazuje na to, že zahrnuje též určitý lidský faktor (sociální arénu).[6]

Kyberprostorem putují nejen běžné maily či komentáře na sociálních sítích, nýbrž také řada citlivých dat, jako jsou údaje o finančních operacích nebo telekomunikační data, a kyberprostor propojuje jednotlivé prvky kritické infrastruktury států.[7] Útoky v kyberprostoru tak představují značné nebezpečí jak pro zájmy jednotlivce, tak pro zájmy státu a společnosti. Nebezpečnost kybernetických útoků jednoznačně dokládají dostupné statistické údaje. Škody, které tyto útoky ročně způsobí, se celosvětově odhadují na 290 bilionů EUR.[8]

2. Evropské a historické souvislosti vládního návrhu

Alarmující statistiky vedou k celosvětové snaze o zajištění kybernetické bezpečnosti. Rovněž Evropská unie reflektuje narůstající potřebu zajištění ochrany kybernetického prostoru. Výchozím dokumentem je Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor, kterou předložila Vysoká předsta-

3) Sněmovní tisk č. 81. Dostupný na http://www.psp.cz/sqw/tisky.sqw?str=3&O=7&PT=K&N=1&F=-N&D=1,2,16&RA=20
4) MACEK, Jakub. Kyberprostor (Cyberspace). Revue pro média. 2003, č. 5. Dostupné na http://rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm
5) ZELINKOVÁ, Věra. Kyberprostor. Dostupné na http://kisk.phil.muni.cz/wiki/Kyberprostor
6) PLECITÝ, V. Kybernetická bezpečnost a trestněprávní postih DodS útoků (útoků odmítnutí služby). Kriminalistika. 2013, roč. XXXXVI, č. 1, s. 3.
7) Ibid., s. 4.
8) CAFOURKOVÁ, T. Cena za kybernetickou bezpečnost. IP&IT Bulletin. 2013, roč. 2, č. 9, s. 8.

vitelka Evropské unie pro zahraniční věci a bezpečnostní politiku.[9] Strategie si klade za cíl především prevenci a zásadní omezení počítačové kriminality, kterého má být dosaženo zavedením pružného a efektivního systému notifikace a reakce na nastalé incidenty a zavedením společné politiky v oblasti počítačové kriminality, a související podporu užívání internetu.[10]

Dne 7. února 2013 Evropská komise předložila návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii.[11] Návrh směrnice vyžaduje, aby každý členský stát přijal národní strategii pro bezpečnost sítí a informací, jmenoval vnitrostátní orgán odpovědný za bezpečnost sítí a informačních systémů a zřídil skupinu pro reakci na počítačové hrozby, tzv. CERT *(Computer Emergency Response Team)*. Návrh dále požaduje, aby odpovědné vnitrostátní orgány spolupracovaly v rámci sítě umožňující bezpečnou a efektivní spolupráci včetně koordinované výměny informací, odhalování incidentů a reakcí na úrovni EU.[12]

Vládní návrh zákona o kybernetické bezpečnosti předjímá to, co směrnice Evropské unie navržená Komisí bude v případě přijetí Radou a Evropským parlamentem po členských státech požadovat. Návrh do parlamentu přichází v době, kdy návrh směrnice je stále v prvním čtení a Evropský parlament o něm dosud nejednal. Mohlo by se tak na první pohled zdát, že Česká republika se snaží být „bruselštější" než Brusel. Skutečnost je ale taková, že vládní návrh se snaží postavit zpátky na nohy to, co je už delší dobu postavené na hlavu.

S rozvojem informačních technologií do České republiky pochopitelně dorazila také počítačová kriminalita. Již na počátku 90. let 20. století na tuto skutečnost zareagovala trestní legislativa. Do nyní již zrušeného zákona č. 140/1961 Sb., trestní zákon, bylo novelou z roku 1991 (zákon č. 557/1991 Sb.) s účinností od 1. ledna 1992 začleněno ustanovení § 257a, jež zavedlo nově skutkovou podstatu trestného činu poškození a zneužití záznamu na nosiči informací. Nepochybně to dokládá, že zákonodárce si byl již v této době dobře vědom nezbytnosti postihovat trestné činy spáchané v kyberprostoru.[13] Nový trestní zákon z roku 2009 pak k postihu počítačové kriminality při-

9) European Commission. Brussels, 7.2.2013. JOIN(2013) 1 final. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Dostupné na http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

10) CAFOURKOVÁ, T.: op. cit. sub 8.

11) Evropská komise. Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. V Bruselu dne 7.2.2013. COM(2013) 48 final. Dostupné na http://ec.europa.eu/transparency/regdoc/rep/1/2013/CS/1-2013-48-CS-F1-1.Pdf Důvodová zpráva k vládnímu návrhu zákona o kybernetické bezpečnosti. Sněmovní tisk č. 81. Dostupný na http://www.psp.cz/sqw/tisky.sqw?str=3&O=7&PT=K&N=1&F=N&D=1,2,16&RA=20 (dále jen „Důvodová zpráva"), s. 18.

12) Důvodová zpráva k vládnímu návrhu zákona o kybernetické bezpečnosti. Sněmovní tisk č. 81. Dostupný na http://www.psp.cz/sqw/tisky.sqw?str=3&O=7&PT=K&N=1&F=N&D=1,2,16&RA=20 (dále jen „Důvodová zpráva"), s. 18.

13) PLECITÝ, V.: op. cit. sub 6, s. 7 - 8.

stoupil mnohem komplexněji.[14] V České republice však stále schází zákonná úprav zaměřená na prevenci zločinů páchaných v kyberprostoru. V tomto směru vládní návrh zákona o kybernetické bezpečnosti rozhodně není předčasný.

Předložení návrhu zákona nepředstavuje první krok ze strany vlády směřujícím k zajištění kybernetické bezpečnosti. Na základě usnesení vlády č. 781 ze dne 19. října 2011 bylo zřízeno Národní centrum kybernetické bezpečnosti jako součást Národního bezpečnostního úřadu. Předmětné usnesení vlády uložilo řediteli Národního bezpečnostního úřadu vybudovat do konce roku 2015 nejen plně funkční Národní centrum kybernetické bezpečnosti, ale i vládní koordinační místo pro okamžitou reakci na počítačové incidenty, tzv. vládní CERT, který bude součástí Národního centra kybernetické bezpečnosti.[15]

3. Zásady vládního návrhu

Vláda jako předkladatel návrhu zákona v důvodové zprávě objasňuje, že návrh vychází ze šesti specifických zásad.

1) Technologická neutralita: Navrhovaná právní úprava důsledně odděluje bezpečnost fungování služeb informační společnosti od informačního obsahu a předmětem regulace tak zde není obsah přenášených informací. Návrh zákona nesměřuje k postihu závadného obsahu šířených informací, např. šíření dětské pornografie, stalkingu nebo porušování práv duševního vlastnictví. Předpokládané povinnosti, které zákon stanoví, se vztahují výhradně k technologickým aspektům fungování služeb informační společnosti. Bezpečnostní opatření, k jejichž dodržování zaváže navrhovaná právní úprava vybrané subjekty, jsou definovány tak, aby mohly být splněny s užitím různých technologií a postupů. Dotčené subjekty budou moci dle vlastního uvážení volit konkrétní způsob zabezpečení jejich informačních struktur.[16]

2) Zajištění ochrany informačního sebeurčení člověka: Pojem informačního sebeurčení člověka zavedl do právní praxe německý Spolkový ústavní soud jako souhrnné označení pro katalog absolutních informačních práv člověka. Informačního sebeurčení zahrnuje na jedné straně pasivní složku, tedy ochranu diskrétní informační sféry, a projevuje se především ochranou soukromí a ochranou osobních údajů. K této pasivní složce přitom v současném chápání pojmu informačního sebeurčení člověka přistupuje aktivní složka, tedy právo aktivně přijímat, zpracovávat a komunikovat informace. Člověk v současném světě nemůže žít plnohodnotný soukromý život bez možnosti komunikovat

14) K tomu viz celk. ŠÁMAL, P. a kol. Trestní zákoník. 2. vyd. Praha: C.H.Beck, 2012, s. 2301 - 2325.
15) Co je to NKBC? Dostupné na http://www.govcert.cz/cs/. Dále viz Důvodová zpráva: op. cit. sub 12, s. 19.
16) Důvodová zpráva: op. cit. sub 12, s. 56 – 57.

s okolním světem[17]. Navrhovaná právní úprava reflektuje právo na informační sebeurčení jako dominantní princip legitimující obecně legislativní zadání k řešení kybernetické bezpečnosti.[18]

3) Ochrana nedistributivních práv: Vláda jako předkladatel návrhu tím má na mysli práva státu na zajištění vnitřní bezpečnosti, na ochranu základních funkcí státu a na ochranu před škodlivými následky výjimečných stavů. Návrh zákona reflektuje skutečnost, že fungování státu je v současné době do značné míry závislé na informačních technologiích. Kybernetický útok může ohrozit nejen právo člověka na informační sebeurčení, nýbrž také fungování státu. V návrhu zákona se to promítá zejména do otázek rozsahu kritické informační infrastruktury a do úpravy kybernetického nebezpečí[19] (viz dále).

4) Minimalizace státního donucení: Povinnosti plynoucí z navržené právní úpravy se zaměřují pouze na ty informační a komunikační systémy, které mají zásadní význam pro naplnění účelu zákona. Povinnost zabezpečit tyto systémy před běžnými formami kybernetických útoků se tak vztahuje pouze na systémy a sítě tvořících kritickou informační infrastrukturu a na významné informační systémy. Nicméně navrhovaná právní úprava zakotvuje možnost dobrovolného zapojení do národního systému kybernetické bezpečnosti pro subjekty provozujících informační systémy, sítě a služby. Zkušenosti ze zahraničí ukazují, že spolupráce s národními dohledovými pracovišti přináší podnikatelským subjektům i akademickému nebo neziskovému sektoru vysoce pozitivní efekty a že zájem o tuto spolupráci bývá velký. Předkládaný návrh volí model provozu národního dohledového pracoviště osobou soukromého práva, a to na základě veřejnoprávní smlouvy.[20]

5) Autonomie vůle regulovaných subjektů: Navrhovaná právní úprava stanovuje pouze základní povinnost a standardní bezpečnostní parametry, přičemž adresátům právních povinností se ponechává volnost ve způsobech, jakými dosáhnou jejich naplnění. Návrh tak reflektuje rozmanitost informačních systémů, služeb a sítí elektronických komunikací, jakož i rozmanitost jejich správců.[21]

6) Bdělost ve vztahu k ostatním státům a k mezinárodnímu společenství: Ačkoliv návrh zákona směřuje primárně k zajištění kybernetické bezpečnosti v rámci České republiky, zohledňuje též zásadu mezinárodního práva označovanou jako „náležitá péče“ (due dilligence)[22], jež státům ukládá povinnost v rámci své

17) V českém prostředí to potvrdil i Ústavní soud. Viz I.ÚS 22/10 ze dne 07.04.2010, N 77/57 SbNU.
18) Důvodová zpráva: op. cit. sub 12, s. 57.
19) Ibid., s. 58.
20) Ibid., s. 58 – 59.
21) Ibid., s. 59.
22) V české literatuře se této zásadě mezinárodního práva věnuje zejm. J. Malenovský. Viz MALENOVSKÝ, J. Mezinárodní právo veřejné. Jeho obecná část a poměr k jiným právním systémům, zvláště k právu českému. 5.

jurisdikce aktivně bránit škodám, které by mohly vzniknout ostatním státům nebo mezinárodnímu společenství. Specifická úprava, která na národní úrovni zabezpečuje informační a komunikační systémy před kybernetickými útoky, totiž chrání tyto systémy i před zneužitím k útokům cíleným mimo českou jurisdikci. [23]

4. Klíčové instituty vládního návrhu

Vládní návrh zákona o kybernetické bezpečnosti ukládá v § 4 odst. 2 specifickou povinnost zavést a provádět bezpečnostní opatření, jakož i vést dokumentaci o těchto opatřeních, a to následujícím orgánům a osobám:

a) Správcům informačních a komunikačních systémů kritické informační infrastruktury - kritickou informační infrastrukturou se v návrhu rozumí prvek nebo systém infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jehož narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu (§ 2 písm. b).

b) Správcům významných informačních systémů - významným informačním systémem se rozumí informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci (§ 2 písm. c).

Bezpečnostním opatřením návrh rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru (§ 4 odst. 1). Rozlišuje přitom opatření organizační a technická (§ 5). Definici bezpečnostních opatření návrh pojímá velmi genericky a předpokládá, že jednotlivá konkrétní řešení bezpečnostních opatření se mohou při současném splnění zákonných požadavků vzájemně odlišovat.

Vládní návrh dále zavádí dva nové instituty – kybernetickou bezpečnostní událost a kybernetický bezpečnostní incident. Kybernetická bezpečnostní událost v podstatě představuje potenciální nebezpečí. Návrh ji v § 7 odst. 1 vymezuje jako událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. Naproti tomu kybernetický bezpečnostní incident už představuje aktuální narušení bezpečnosti. V § 7 odst. 2 je vymezen jako narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

Vyd. Brno: Doplněk, 2008, s. 320 a 349.
23) Důvodová zpráva: op. cit. sub 12„ s. 60.

Pokud jde o kybernetické bezpečnostní události, návrh zakotvuje pouze povinnost tyto události detekovat, a to správcům významných sítí, správcům informačních a komunikačních systémů kritické informační infrastruktury a správcům významného informačního systému (§ 7 odst. 3). V případě kybernetických bezpečnostních incidentů má stejný okruh správců – s výjimkou správců významných sítí - povinnost hlásit každý takový incident Národnímu bezpečnostnímu úřadu, který vede jejich evidenci. Správcové významných sítí hlásí kybernetické bezpečnostní incidenty provozovateli národního CERT (§ 8).

Vládní návrh zákona zakotvuje právo Národního bezpečnostního úřadu vydávat opatření, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu (§ 11 odst. 1). Za běžného režimu, tedy pokud není vyhlášen stav kybernetického nebezpečí, mají povinnost přímo aplikovat opatření jen vybrané typy orgánů a osob, tj. správci informačních a komunikačních systémů zařazených do kritické informační infrastruktury a správci významných informačních systémů. Pouze při vyhlášení stavu kybernetického nebezpečí se povinnost aplikovat opatření rozšíří i na ostatní orgány a osoby (§ 11 odst. 3 a 4). Opatřeními přitom jsou:

Varování: Národní bezpečnostní úřad je vydá, pokud se dozví o hrozbě v oblasti kybernetické bezpečnosti. Zveřejní je na svých internetových stránkách a oznámí dotčeným orgánům a osobám (§ 12).

Reaktivní opatření: Slouží k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem (§ 13).

Ochranné opatření: Slouží ke zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací. Národní bezpečnostní úřad je uloží na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu (§ 14).

Navrhovaná právní úprava počítá se zřízením dvou dohledových pracovišť, a to národního a vládního CERT, jejichž úkolem bude vyhodnocování kybernetické bezpečnostní situace v informačních a komunikačních systémech a ochrana těchto systémů před kybernetickými bezpečnostními incidenty.

Vládní CERT bude působit jako součást Národního bezpečnostního úřadu. Jako orgán veřejné moci bude disponovat nařizovacími a sankčními pravomocemi na úseku kybernetické bezpečnosti, a to včetně kontrolních a sankčních pravomocí. Vzhledem k zásadě technologické neutrality a zásadě minimalizace státního donucení budou ovšem jeho pravomoci omezeny. V podstatě bude přímo působit pouze na vybrané in-

formační a komunikační systémy, které mají zásadní význam pro národní zájmy České republiky, tedy na oblast kritické informační infrastruktury a významných informačních systémů (§ 20).

Naproti tomu národní CERT má odpovídat na poptávku osob soukromého práva po centralizovaném soukromoprávním řešení sběru informací o kybernetické bezpečnosti a na potřebu metodické pomoci při účinnému řešení různých typů kybernetických bezpečnostních incidentů v informačních a komunikačních systémech, které nemají zásadní význam pro národní zájmy České republiky. Národní CERT nebude disponovat žádným mocenským oprávněním, nýbrž bude svoje služby nabízet subjektům, které aktivně projeví zájem o výhody kolektivní ochrany před kybernetickými bezpečnostními incidenty. Provozovatelem národního CERT bude právnická osoba vázaná veřejnoprávní smlouvou uzavřenou s Národním bezpečnostním úřadem (§ 18).

Vládní návrh zákona dále upravuje vyhlašování stavu kybernetického nebezpečí. Podle § 21 odst. 1 se stavem kybernetického nebezpečí bude rozumět stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací. Stav kybernetického nebezpečí bude vyhlašovat ředitel Národního bezpečnostního úřadu, a to na dobu nezbytně nutnou, nejdéle na 7 dnů. Uvedenou dobu může ředitel Národního bezpečnostního úřadu prodloužit, souhrnná doba trvání vyhlášeného stavu kybernetického nebezpečí však nesmí překročit 30 dnů. Rozhodnutí o vyhlášení stavu kybernetického nebezpečí se bude vyhlašovat vyvěšením na úřední desce Národního bezpečnostního úřadu a informace o jeho vyhlášení se bude zveřejňovat v celoplošném rozhlasovém a televizním vysílání. V průběhu vyhlášeného stavu kybernetického nebezpečí ředitel Úřadu informuje vládu o postupech při řešení stavu kybernetického nebezpečí a o aktuálním stavu hrozeb, které vedly k vyhlášení stavu kybernetického nebezpečí (§ 21 odst. 2,3 a 4).

V případě, že vládní návrh bude přijat, stav kybernetického nebezpečí se tak přiřadí ke stávajícím čtyřem výjimečným stavům, s jejichž vyhlašováním počítá stávající právní úprava (jedná se o válečný stav, stav ohrožení státu, nouzový stav a stav nebezpečí).

5. Možná úskalí

Hlavní úskalí navrhovaného zákona vidím v jeho nákladech. Jak už jsem poukázal výše v tomto článku, vládní návrh zákona o kybernetické bezpečnosti předjímá to, co v případě přijetí bude po členských státech požadovat směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. Evropská Komise jako předkladatel návrhu směrnice vyčíslila poměrně podrob-

ně náklady, které si zavedení směrnice vyžádá.[24] Jsem přesvědčený, že toto vyčíslení je relevantní i při projednávání vládního návrhu zákona o kybernetické bezpečnosti v rámci České republiky.

Návrh směrnice kráčí cestou zapojení fyzických a právnických osob do zajišťování kybernetické bezpečnosti. To nepochybně odpovídá současnému trendu. Uznává se totiž, že bez zapojení fyzických a právnických osob nelze v současném světě dosáhnout komplexního zajištění bezpečnosti.[25] Jenže zapojení soukromých fyzických a právnických osob často znamená také přenášení nákladů. Je nepochybné, že směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii přenáší část nákladů na soukromý sektor.[26] Evropská komise vyčíslila, že malé a střední podniky budou muset na uvedení svých informačních systémů do souladu se směrnicí vynaložit 2 500 - 5 000 EUR.[27] Pro řadu drobných podniků to určitě není zanedbatelná částka. Nezbytnost vynaložit tyto náklady tak může přibrzdit hospodářský růst.

Vládní návrh zákona o kybernetické bezpečnosti v zásadě kráčí stejnou cestou jako návrh směrnice Evropské unie. I zde nepochybně bude docházet k přenášení nákladů na soukromý sektor. Vláda jako předkladatel návrhu se sice v důvodové zprávě věnuje rozboru nákladů a přínosů, ovšem žádná konkrétní čísla neuvádí.[28] Téměř to působí dojmem, jakoby vláda neměla jasnou představu, jaké náklady navržený zákon skutečně bude vyžadovat.

Ve vládním návrhu zákona o kybernetické bezpečnosti spatřuji ještě jedno možné úskalí. Jak jsem poukázal výše, návrh má zavést do českého právního řádu nový výjimečný stav, a to stav kybernetického nebezpečí. Schází zde ovšem pojistka proti zneužití. Srovnáme-li navrženou úpravu, se stávající úpravou vyhlašování výjimečných stavů, najdeme jeden podstatný rozdíl. Válečný stav a stav ohrožení státu vyhlašuje parlament jako zastupitelský sbor volený přímo občany (čl. 43 odst. 1 Ústavy ČR a čl. 7 odst. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR). Toto rozhodnutí parlamentu sice nepodléhá žádnému přezkumu, avšak vzhledem k tomu, že parlament představuje nejvyšší zastupitelský sbor nelze v tom spatřovat nebezpečí. Nouzový stav vyhlašuje vláda jak vrcholný orgán moci výkonné (čl. 5 odst. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR), ovšem Poslanecká sněmovna může toto vyhlášení zrušit (čl. 5 odst. 4 ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR). V případě stavu kybernetického nebezpečí, který vyhlašuje ředitel Národního bezpečnostního úřadu, tedy ředitel orgánu moci výkonné, podobná pojistka proti případnému zneužití ve vládním návrhu zákona o kybernetické bezpečnosti zakotvena chybí. Je zde sice určitá podobnost se stavem nebezpečí, který podle § 3 odst. 3 zákona 240/200 Sb., o krizovém řízení, vyhlašuje hejtman kraje, přičemž jiný orgán nemá pravomoc toto vyhlášení zrušit, avšak

24) COMMISSION STAFF WORKING DOCUMENT. IMPACT ASSESSMENT. 13 February 2013, SWD(2013) 32 final (dále jen „Commission Working Document“)
25) K tomu viz např. PROCHÁZKOVÁ, D.: op. cit sub 1, s. 30.
26) K tomu viz celk. CAFOURKOVÁ, T.: op. cit. sub 8, s. 9 - 10.
27) Commission Working Document: op. cit. sub 24, p. 53.
28) Důvodová zpráva: op. cit. sub 12, s. 37 – 47.

stav nebezpečí se vyhlašuje pouze pro území daného kraje nebo jeho část, zatímco stav kybernetického nebezpečí se vyhlašuje pro celé území České republiky.

Závěr

Vládní návrh zákona o kybernetické bezpečnosti usiluje o zaplnění významné mezery v českém právním řádu, neboť by se měl stát prvním předpisem zaměřeným na prevenci útoků v kyberprostoru a na celkové zajištění kybernetické bezpečnosti. Návrh předjímá to, co v případě přijetí bude po členských státech Evropské unie požadovat směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací, jejíž návrh se v evropských strukturách projednává. Ze všech těchto důvodů je přijetí návrhu více než žádoucí.

Vládní návrh stanovuje povinnost přijmout bezpečnostní opatření vybraným orgánům a osobám a dále zavádí dva nové instituty – kybernetickou bezpečnostní událost, jež představuje potenciální nebezpečí, a kybernetický bezpečnostní incident spočívající v aktuálním narušení kybernetické bezpečnosti. V případě přijetí návrhu získá Národní bezpečnostní úřad nové významné pravomoci, a to právo vydávat opatření k zajištění kybernetické bezpečnosti a právo vyhlašovat stav kybernetického nebezpečí. Návrh v neposlední řadě počítá se zřízením dvou dohledových pracovišť, a to národního a vládního CERT.

Ačkoliv vládní návrh zavádí řadu potřebných institutů, je možné v něm identifikovat některá úskalí. Zvolený model zajišťování kybernetické bezpečnosti znamená přenášení části nákladů na soukromý sektor, což může přibrzdit ekonomický růst. Vláda jako předkladatel návrhu se s tímto v důvodové zprávě nijak nevypořádala. Pokud jde o nové pravomoci Národního bezpečnostního úřadu, schází v návrhu pojistka proti jejich zneužití.

Literatura

Knihy

[1] MALENOVSKÝ, J. Mezinárodní právo veřejné. Jeho obecná část a poměr k jiným právním systémům, zvláště k právu českému. 5. Vyd. Brno: Doplněk, 2008. ISBN 978-80-210-4474-6

[2] PROCHÁZKOVÁ, D. Bezpečnost, krizové řízení a udržitelný rozvoj. Praha: Univerzita Jana Amose Komenského Praha, 2010. ISBN 978-80-86723-97-6

[3] ŠÁMAL, P. a kol. Trestní zákoník. 2. vyd. Praha: C.H.Beck, 2012. ISBN 978-80-7400-428-5

Články

[4] CAFOURKOVÁ, T. Cena za kybernetickou bezpečnost. IP&IT Bulletin. 2013, roč. 2, č. 9, s. 8 – 10.

[5] DWORZECKI, Jacek. Bezpečnost státu jako součást udržitelného rozvoje. In BÍLÝ, J. a kol. Veřejná správa a bezpečnost státu jako součást udržitelného rozvoje. České Budějovice: Vysoká škola evropských a regionálních studií, 2013, s. 97 – 105. ISBN 978-80-87472-48-4

[6] MACEK, Jakub. Kyberprostor (Cyberspace). Revue pro média. 2003, č. 5. Dostupné na http://rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm

[7] PLECITÝ, V. Kybernetická bezpečnost a trestněprávní postih DodS útoků (útoků odmítnutí služby). Kriminalistika. 2013, roč. XXXXVI, č. 1, s. 3 – 21. ISSN1210-9150

[8] ZELINKOVÁ, Věra. Kyberprostor. Dostupné na http://kisk.phil.muni.cz/wiki/Kyberprostor

Další zdroje

[9] Parlament ČR. Poslanecká sněmovna. Sněmovní tisk č. 81. Dostupný na http://www.psp.cz/sqw/tisky.sqw?str=3&O=7&PT=K&N=1&F=N&D=1,2,16&RA=20

[10] European Commission. Brussels, 7.2.2013. JOIN(2013) 1 final. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Dostupné na http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[11] Evropská komise. Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. V Bruselu dne 7.2.2013. COM(2013) 48 final. Dostupné na http://ec.europa.eu/transparency/regdoc/rep/1/2013/CS/1-2013-48-CS-F1-1.Pdf

[12] COMMISSION STAFF WORKING DOCUMENT. IMPACT ASSESSMENT. 13 February 2013, SWD(2013) 32 final

[13] Co je to NKBC? Dostupné na http://www.govcert.cz/cs/

[14] I.ÚS 22/10 ze dne 07.04.2010, N 77/57 SbNU